УДК 681.3.06

ПРЕДСТАВЛЕНИЕ ЭЛЕМЕНТОВ ЯКОБИАНА ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ РОДА ДВА

Бессалов А.В., Третьяков Д.Б.

Введение

Для решения задач гиперэллиптической криптографии обсуждается вопрос представления дивизора гиперэллиптической кривой рода 2 *парой точек в расширении основного поля. Раскрывается изоморфная связь между парами сопряженных точек и полиномами приведенного дивизора в форме Мамфорда*

Сегодня все стандарты асимметричной криптографии базируются на арифметике абелевой группы точек эллиптической кривой над конечным полем. Эллиптическая криптография, кроме традиционных криптосистем, основанных на проблеме дискретного логарифмирования на эллиптической кривой, стала основой для построения криптосистем с новыми свойствами. В частности, в последние два десятилетия были предложены криптосистемы на гиперэллиптических кривых [1], и криптосистемы, основанные на спариваниях точек эллиптических кривых [2]. Гиперэллиптические кривые – это кривые более высокого рода, которые являются обобщением понятия эллиптической кривой. При этом, если билинейная криптография ведет в сторону сверхбольших полей (до десятков килобит), то гиперэллиптические кривые дают реальную перспективу использовать малые поля (десятки бит). Ясно, что такая перспектива является привлекательной, и поэтому активно исследуется учеными мира.

Точки гиперэллиптической кривой, в отличие от точек эллиптической кривой, не образуют группу. Формальные суммы точек называются дивизорами. Количество входящих в дивизор точек называют весом дивизора. В качестве групповой структуры рассматривается якобиан кривой, который представляет собой факторгруппу дивизоров нулевой степени по подгруппе главных дивизоров (дивизоров функций) [3]. Представителем каждого класса рассматриваемой факторгруппы является приведенный дивизор, который может быть записан в виде двух полиномов в форме Мамфорда [4]. Аналогично операции сложения точек эллиптической кривой введена операция сложения дивизоров гиперэллиптической кривой, которая, однако, является гораздо более сложной [5].

Естественно было ожидать, что более сложный математический аппарат может повысить безопасность криптосистемы. Однако при всей сложности аппарата очень скоро стало известно, что гиперэллиптические кривые подвержены атаке исчисления индексов. При этом проблема дискретного логарифмирования из экспоненциальной упрощается до субэкспоненциальной. Причем эффективность такой атаки растет с возрастанием рода кривой. В этой связи сегодня наиболее перспективными для криптографических приложений считаются кривые рода 2 и 3.

Для разработчиков криптосистем одним из приоритетов всегда является вопрос эффективности. Основная задача при этом - сократить объем используемой памяти и увеличить скорость криптографических преобразований. С целью увеличения скорости преобразований исследования ведутся в направлении оптимизации групповой операции. Разными разработчиками представлены явные формулы сложения и удвоения дивизоров (например [6,7]).

Что касается памяти, сразу же возникает вопрос: каким образом записывать элемент (дивизор) гиперэллиптической кривой? Оказывается, он имеет размер, например,

для кривой второго рода, в два раза превосходящий размер элемента для эллиптической кривой. Если точка эллиптической кривой имеет две координаты (x, y), то для хранения дивизора уже нужно хранить четыре параметра. Каждый из них имеет размер в два раза меньше координаты точки эллиптической кривой, но в общей сложности он остается таким же.

Целью данной статьи является исследование возможности оптимизации представления дивизора гиперэллиптической кривой второго рода с помощью координат входящих в него точек.

Представление дивизора гиперэллиптической кривой

Каждый элемент якобиана гиперэллиптической кривой, определенной над $GF(p)$, представляется двумя полиномами в форме Мамфорда с коэффициентами из $GF(p)$. Однако координаты точек, входящих в дивизор, в этом случае определены в $GF(p^g)$. Рассмотрим связь между точками, входящими в дивизор, и его представлением парой полиномов.

Пусть имеем гиперэллиптическую кривую

$$C: \quad y^2 + h(x)y = f(x),$$

для которой полиномы $h(x)$, $f(x)$ со степенями $\deg h(x) < g$, $\deg f(x) = 2g + 1$ определены над полем $\mathbf{F}_p$, $p > 3$. Рассмотрим кривую рода $g = 2$ со старшей степенью $\deg f(x) = 5$. Координаты точки (X,Y) кривой C, определяющие якобиан гиперэллиптической кривой (ГЭК) рода 2, лежат в поле $\mathbf{F}_p$ и в расширении $\mathbf{F}_p^2$. Справедливо

Утверждение 1. Для любой точки $P = (X,Y)$ в расширении $\mathbf{F}_p^2$ существует сопряженная точка $\widetilde{P} = (\widetilde{X}, \widetilde{Y})$, такая, что приведенный дивизор их суммы в форме Мамфорда

$$D[P + \widetilde{P}] = < a(x), b(x) > \tag{1}$$

однозначно представляется параболой и уравнением прямой

$$a(x) = (x - X)(x - \widetilde{X}) = x^2 + Ax + B, \tag{2}$$

$$b(x) = Y\frac{x - \widetilde{X}}{X - \widetilde{X}} + \widetilde{Y}\frac{x - X}{\widetilde{X} - X} = Gx + H, \tag{3}$$

где коэффициенты $A, B, G, H \in \mathbf{F}_p$. Полином $a(x)$ несет информацию об x-координатах точек P и $\widetilde{P}$, а $b(x)$ – об их y-координатах.

Доказательство. Пусть известны координаты точки $P = (X,Y)$ в расширении $\mathbf{F}_p^2$ с неприводимым полиномом $\psi(x) = t^2 + a_1 t + a_0$

$$X = ct + d, \qquad Y = et + f. \quad c, e \neq 0. \tag{4}$$

Определим координаты сопряженной точки

$$\widetilde{X} = \widetilde{c}t + \widetilde{d}, \quad \widetilde{Y} = \widetilde{e}t + \widetilde{f}. \tag{5}$$

Из (2) следует

$$X + \tilde{X} = (c + \tilde{c})t + d + \tilde{d},$$
$$X\tilde{X} = (c\tilde{c}t^2 + (c\tilde{d} + \tilde{c}d)t + d\tilde{d}) \bmod \psi(t).$$

Так как правые части этих равенств лежат в поле $\mathbf{F}_p$, то отсюда следует

$$\tilde{c} = -c \bmod p,$$
$$\frac{\tilde{d} - d}{c} = -a_1 \bmod p \Rightarrow \quad \tilde{d} = (d - a_1 c) \bmod p.$$

Подставляя эти параметры в (5), легко выразить координаты сопряженной точки как

$$\tilde{X} = X(\tau) = c\tau + d, \quad \tilde{Y} = Y(\tau) = e\tau + f, \tag{6}$$

с линейной заменой переменной

$$\tau = (-t - a_1) \bmod p\,. \tag{7}$$

Таким образом, точки P и $\tilde{P}$ связаны простой заменой переменной. Ясно, что для каждой точки P в расширении $\mathbf{F}_p{}^2$ существует единственная сопряженная точка $\tilde{P}$, и эта пара точек единственным образом определяет полиномы (2) и (3) приведенного дивизора (1). Доказательство завершено.

Обратная задача – нахождение координат точек P и $\tilde{P}$ при заданном в полиномиальной форме дивизоре – требует на первом этапе решения квадратного уравнения в правой части (2) в расширении $\mathbf{F}_p{}^2$. Дискриминант этого уравнения

$$\Delta = (A^2 - 4B) \bmod p \tag{8}$$

является квадратичным вычетом или невычетом в поле $\mathbf{F}_p$. В первом случае получаем x-координаты двух точек кривой $\mathbf{C}$ над $\mathbf{F}_p$

$$X_{1,2} = \frac{-A \pm \sqrt{\Delta}}{2}, \tag{9}$$

во втором случае – координаты сопряженных точек кривой C над расширением $\mathbf{F}_p{}^2$. Выразим в последнем случае

$$\Delta = (\alpha t + \beta)^2 mod\ (t^2 + a_1 t + a_0) = \alpha^2(a_1{}^2/4 - a_0) \bmod p.$$

Отсюда определяем

$$\beta = \frac{a_1 \alpha}{2} \bmod p,$$
$$\alpha^2 = \frac{4\Delta}{a_1{}^2 - 4a_0} \bmod p \tag{10}$$

Тогда с учетом равенства $\sqrt{\Delta} = \alpha(t + \frac{a_1}{2})$ получим x-координаты сопряженных точек P и $\tilde{P}$

$$X = \frac{-A+\alpha(t+\frac{a_1}{2})}{2}, \quad \tilde{X} = \frac{-A-\alpha(t+\frac{a_1}{2})}{2} \tag{11}$$

Их у-координаты легко находятся из равенств

$$Y = b(X), \qquad \tilde{Y} = b(\tilde{X}). \tag{12}$$

Пример 1. Рассмотрим кривую 2-го рода $y^2 = (x^5 + 2x^2 + x + 3)\text{mod}7$ с неприводимым полиномом $\psi(x) = t^2 - t - 1$ ($a_1 = -1$) в расширении $\mathbf{F}_p{}^2$. Для известной точки $P = (5t + 6, 2t + 4)$ найдем сопряженную точку $\tilde{P}$ и приведенный дивизор их суммы. Согласно (6) и (7) имеем

$$\tilde{X} = X(\tau) = 5\tau + 6 = 5(-t+1) + 6 = 2t + 4,$$
$$\tilde{Y} = Y(\tau) = 2\tau + 4 = 2(-t+1) + 4 = 5t + 6.$$

Тогда согласно (2), (3) и с учетом

$$A = -(X + \tilde{X}) = -(6 + 4) = 4,$$
$$B = X\tilde{X} = (5t+6)(2t+4) \bmod (t^2 - t - 1) = (3t^2 - 3t + 3) \bmod (t^2 - t - 1) = 6$$

дивизор (1) суммы точек P и $\tilde{P}$ в форме Мамфорда определяется полиномами

$$a(x) = (x - 5t - 6)(x - 2t - 4) = x^2 + 4x + 6,$$
$$b(x) = (2t+4)\frac{x-(2t+4)}{(5t+6)-(2t+4)} + (5t+6)\frac{x-(5t+6)}{(2t+4)-(5t+6)} = 6x + 3,$$

Решим теперь обратную задачу – по известному дивизору найдем координаты сопряженных точек P и $\tilde{P}$. В нашем примере согласно (8) $\Delta = A^2 - 4B = 6$ является квадратичным невычетом в поле F_7. В расширенном поле можно найти квадратичный вычет в форме $\sqrt{\Delta} = \alpha(t + \frac{a_1}{2})$. Из (10) имеем

$$\alpha^2 = \frac{4*6}{1+4} \bmod 7 = 2, \quad \alpha = 3.$$

Тогда в соответствии с (11)

$$X = \frac{-4+3(t-\frac{3}{2})}{2} \bmod 7 = \frac{-4+3(t-4)}{2} \bmod 7 = 5t + 6,$$
$$\tilde{X} = \frac{-4-3(t-4)}{2} \bmod 7 = 2t + 4.$$

С помощью (12) находим у-координаты сопряженных точек

$$Y = 6X + 3 = 2t + 4, \qquad \tilde{Y} = 6\tilde{X} + 3 = 5t + 6.$$

Как видим, обратные вычисления дают значения координат точек P и $\widetilde{P}$.
При $c = 0$ и $e = 0$ в (4) координаты точек лежат в основном поле $\mathbf{F}_p$, при этом сопряженные точки совпадают $P = \widetilde{P}$, а дивизор их суммы отвечает удвоению точки P. Кроме того, над основным полем $\mathbf{F}_p$ формируются элементы якобиана, представляющие всевозможные пары различных не противоположных точек **C**, определенных над этим полем, а также дивизоры веса 1, представляющие каждую одну такую точку. Отсюда следует, что пара точек кривой **C** и элементы ее якобиана изоморфны лишь над расширением $\mathbf{F}_p^2$. Заметим, однако, что при больших значениях модуля p, характерных для криптографических приложений, число точек **C** над расширением приблизительно в p раз преобладает над числом точек кривой, определенных над основным полем $\mathbf{F}_p$. Это значит, что и элементы якобиана кривой в основном формируются на основе пар точек над расширением $\mathbf{F}_p^2$.

Заключение

Для записи элемента якобиана гиперэллиптической кривой второго рода в виде полиномов $a(x)$ и $b(x)$ требуется 4 параметра $A, B, G, H \in \mathbf{F}_p$ (см. (2),(3)) общей длиной $4\log p$. Такой же размер имеет информация о двух координатах (X,Y) точки эллиптической кривой приблизительно того же порядка, что и у якобиана ГЭК-2. Представление дивизора с помощью одной точки из пары P, $\widetilde{P}$ не дает выигрыша в памяти, так как координаты точки над расширением $\mathbf{F}_p^2$ опять имеют общий размер $4\log p$.

Для гиперэллиптической кривой третьего рода дивизор может состоять из трех, двух или одной точки. Приведенные выше аналитические соотношения в этом случае уже не работают. Для представления элемента якобиана необходимо хранить уже 6 параметров. Но при этом надо учитывать, что сами параметры имеют меньшую длину.

В общем случае, для гиперэллиптической кривой рода g в дивизор может входить максимум g точек. Для хранения одного элемента необходимо выделить память $2g \log p$ бит. С учетом того, что при сохранении одинакового уровня стойкости размер основного поля можно уменьшить пропорционально роду кривой, объем требуемой памяти приблизительно равен $2g (\log n)/g = 2 \log n$, где n - порядок якобиана. Ясно, что он не зависит от рода кривой, а определяется только выбранным уровнем стойкости.

Сократить объем требуемой памяти можно в том случае, если использовать дивизор веса 1 (для одной точки над полем $\mathbf{F}_p$), например, в качестве генератора якобиана.

Литература

1. *N. Koblitz. Hyperelliptic cryptosystem / N. Koblitz // Journal of Crypto. – 1989. – № 1. – P. 139-150.*
2. *Boneh D. Short signatures from the Weil pairing. / D.Boneh, H.Shacham, B.Linn./ Advances in Cryptology – ASIACRYPT 2001, Springer-Verlag, 2001/ - pp.514-532.*
3. *Menezes A. An Elementary Introduction to Hyperelliptic Curves [Электронный ресурс] / Menezes A., Wu Y., Zuccherato R. : Published as Technical Report CORR 96-19 Department of C&O University of Waterloo : Ontario : Canada,– 1996.- P. 1-35. – Режим доступа: www.cacr.math.uwaterloo.ca/techreports/1997/corr96-19.ps*
4. *Мамфорд Д. Лекции о тэта-функциях / Д. Мамфорд. – М.: Мир. –1988. – 448 с.*
3. *Cantor D.G. Computing in the Jacobian of a hyperelliptic curve / D.G. Cantor // Math. Comp. 48, 177. – 1987. – P. 95-101.*
5. *Wollinger T. Fast explicit formulae for genus 2 hyperelliptic curves using projective coordinates (Updated) [Электронный ресурс] / T. Wollinger, V. Kovtun // Cryptology ePrint Archive, Report 2008/056. – 2003. – Режим доступа: http://eprint.iacr.org/2008/056.pdf.*
6. *Wollinger T. Software and Hardware Implementation of Hyperelliptic Curve Cryptosystem : Dissertation for the Degree of Doctor-Ingenious / T. Wollinger. – Bochum. – Germany, – 2004. – 201 p.*